

REMARKS

Claims 1-32 are pending in the application. Claim 1 is amended. Claims 1 - 32 remain for consideration.

Claim Rejections – 35 USC §102

The Examiner rejects claims 1-32 as being anticipated by Walker et al. (U.S. Patent No. 6,163,771). The Examiner states that:

Claims 1-32 have been rejected under the newly found prior Walker, Walker discloses a mail-order based credit card fraud, both Visa and MasterCard have deployed databases that allow a merchant to verify that a given credit card account number is connected to a specific billing address. Visa calls this service the Address verification service, The theory behind the service is that a thief (for example, a dishonest restaurant waiter) might be able to use a credit card receipt slip to steal an active account number, but if he tries to use that number for a mail order purchase he would not know the correct address associated with that number. Even if a thief were to obtain the cardholder's address, this service can allow a merchant to compare the shipping address of the catalog order to the current billing address for that account number and thus possibly identify any suspicious activity (which is readable as Applicant's claimed invention wherein said a method for detecting fraud non-personal transactions), comprising the steps of: Collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to-address; transmitting said ship-to-address to a fraud-detection system, processing said ship-to-address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to-address against criteria, and returning the relative risk of fraudulent activity associated with the transaction (see, col 2, lines 7-20).

The Examiner's above example involving the dishonest waiter is illustrative in showing the inadequacy of existing methods of fraud detection and will, hopefully, provide the Applicant with an opportunity to more clearly explain the Applicant's invention. In the above example, which is elaborated upon, below, a dishonest waiter somehow obtains both a credit card account number and the cardholder's address. With this information, the dishonest waiter goes home and, e.g., orders a new stereo from an online electronics store. Presumably, the fact that the (cardholder's) billing address is different from the (dishonest waiter's home address) shipping address identifies the transaction as possibly suspicious.

A flaw in the above system is that the above suspicious transaction is indistinguishable from, reportedly, up to 30% of all legitimate transactions. As an example, it is common practice for an honest patent attorney to use his credit card to order products over the internet at the office during the lunch hour. The billing address of the credit card is the honest patent attorney's home address. However, since no one is at home during delivery hours, the honest patent attorney has the products shipped to his office, or perhaps ships a gift directly to a gift recipient. In this common scenario, the billing address and the shipping address are different, even though the transaction is completely legitimate. Thus, it can be seen that a "billing address different from shipping address" test flags so many legitimate transactions as potentially fraudulent that such a test is virtually worthless.

Applicant's method for fraud detection differs from the method cited by Walker and from the method described in the above two examples because Applicant's method *does not utilize the billing address as a criteria to be checked against the shipping address.*

Applicant's base claim 1 is amended to clarify that the step of checking the purchaser's ship-to address involves checking the ship-to address against non-billing address criteria. Instead of utilizing the billing address, Applicant's invention involves checking the purchaser's ship-to address against a database "to determine whether the purchase's ship-to address exists" (claim 3); "comparing a zip code of the ship-to address against a post office database" (claim 4); comparing the city and state of the ship-to address against the city and state with a ZIP + 4 code (claim 6); checking against "the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address" (claim 7); against "the national change of address service database or the publisher's change of address database (claim 8); against a rating for a building site "to determine whether the building or lot type is inconsistent with the transaction data" (claim 9); against "an historical database to determine whether a prior history of fraud exists (claim 10); against "a modeling engine to determine which element exists in the demographic data which correlate with fraudulent trends (claim 16); etc. None of the above listed claims further define the "criteria" of claim 1 as having anything to do with the

“billing address”. As such, Applicant’s method is wholly distinct from the cited art.

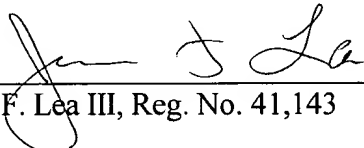
For at least the above reasons, Applicant request allowance of the claims over the cited art.

Considering the foregoing, it is sincerely believed that this case is in condition for allowance, which is respectfully requested.

This paper is intended to constitute a complete response to the outstanding Office Action. Please contact the undersigned if it appears that a portion of this response is missing or if there remain any additional matters to resolve. If the Examiner feels that processing of the application can be expedited in any respect by a personal conference, please consider this an invitation to contact the undersigned by phone.

Respectfully submitted,

Date: 8-25-06


James F. Lea III, Reg. No. 41,143

FELLERS, SNIDER, BLANKENSHIP,
BAILEY & TIPPENS, P.C.
321 South Boston, Suite 800
Tulsa, Oklahoma 74103-3318
(918) 599-0621

Customer Number: 22206

ATTORNEYS FOR APPLICANT